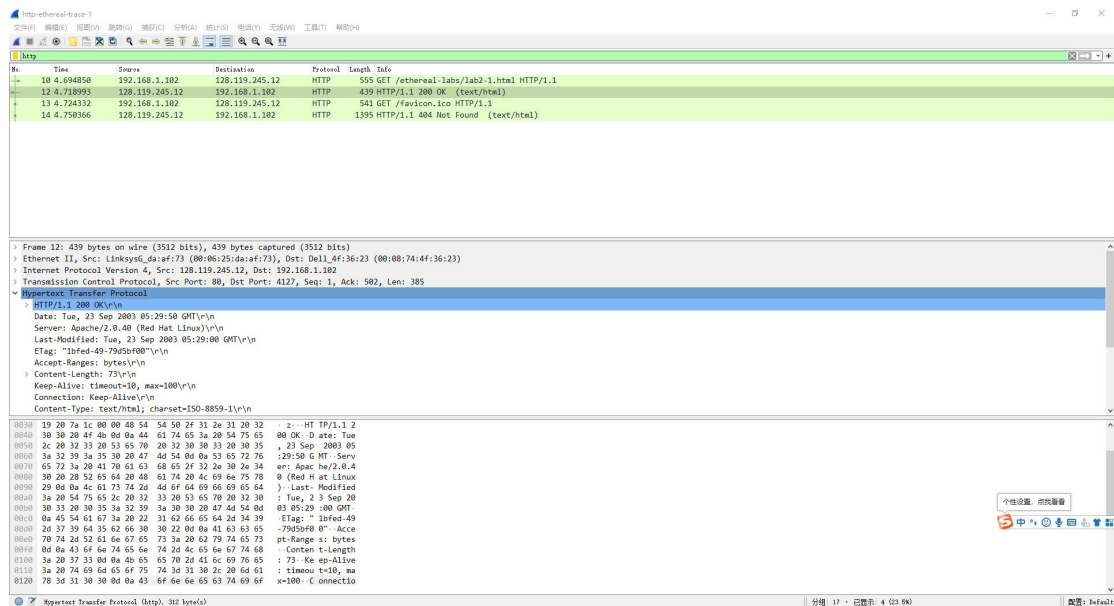


## Lab Exercise 2: HTTP & Socket Programming

### z529005 LongHao

### Exercise 3: Using Wireshark to understand basic HTTP request/response messages

#### Question 1



The status code is 200 and phrase is OK.

#### Question 2

Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n

Server: Apache/2.0.40 (Red Hat Linux)\r\n

Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n

The last modified data of browser is Tue, 23 Sep 2003 05:29:00 GMT.

Yes, the response also contain a DATE header which is Tue, 23 Sep 2003 05:29:00 GMT.

The different is that the DATE header is when the request is sent to the client but the last modified is the time when HEML file was changed.

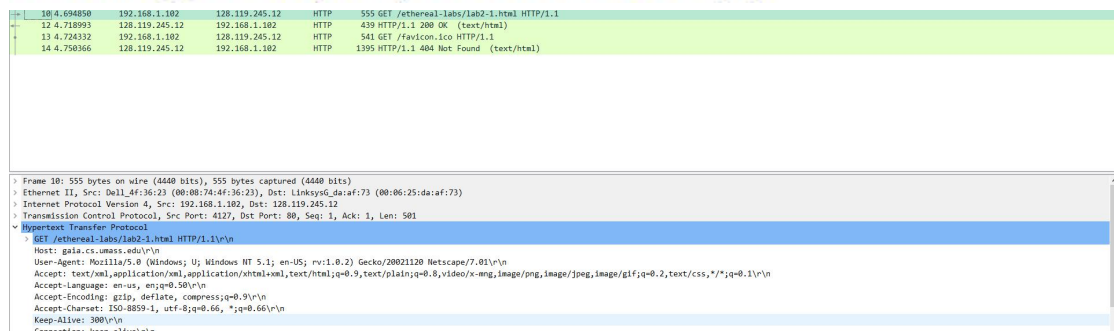
#### Question 3

Content-Length: 73\r\n

Keep-Alive: timeout=10, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=ISO-8859-1\r\n



The connecting is persistent because the header of Connecting is Keep-Alive and the default

setting is persistent.

#### Question 4

**Content-Length: 73\r\n**

There are 73 bytes of content are being returned to the browser.

#### Question 5

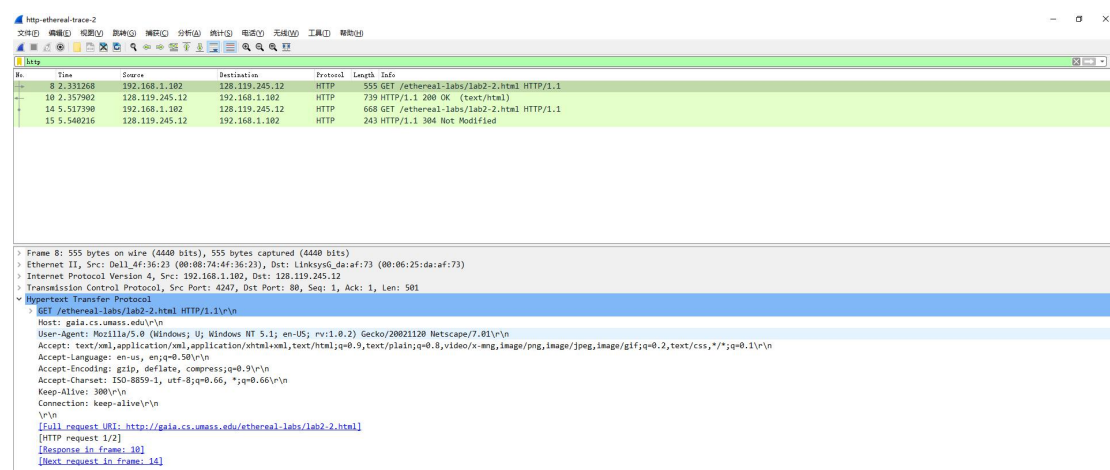
Line-based text data: text/html (3 lines)

```
<html>\n
Congratulations. You've downloaded the file lab2-1.html!\n
</html>\n
```

The data contained inside the HTTP response packet is a text file.

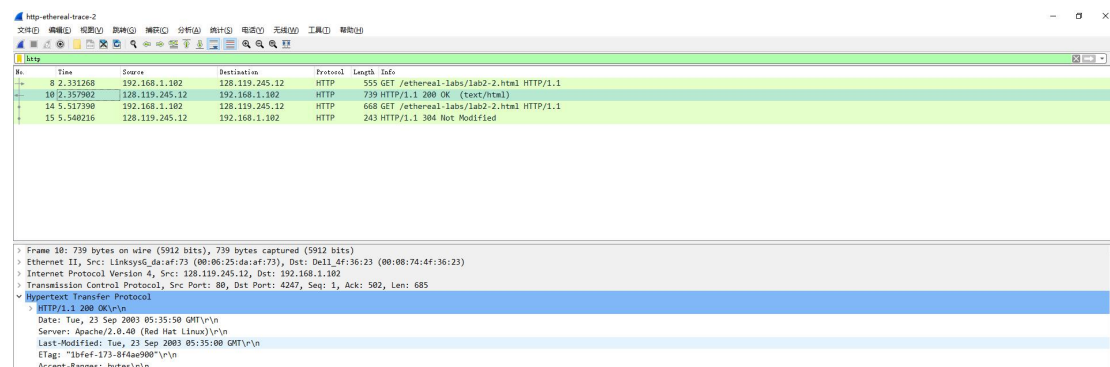
## Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction

#### Question 1



No, I don't see an "IF-MODIFIED-SINCE" line in the HTTP GET.

#### Question 2



Yes, the response indicate the last time that the requested file was modified

#### Question 3

http-ethereal-trace-2

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.337902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.537390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.548216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Frame 14: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits)

Ethernet II, Src: Dell\_Af:36:23 (00:08:74:df:36:23), Dst: Linksys6\_da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614

Hypertext Transfer Protocol

GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,\*/\*;q=0.1\r\n

Accept-Language: en-us,en;q=0.50\r\n

Accept-Encoding: gzip, deflate, compress;q=0.9\r\n

Accept-Charset: ISO-8859-1, utf-8;q=0.66,\*q=0.66\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n

If-None-Match: "1bfef-173-8f4ae900"\r\n

Cache-Control: max-age=0\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]

[HTTP request 2/2]

[Prev request in frame: 8]

[Response in frame: 33]

0000 00 06 25 da af 73 00 08 74 df 36 23 08 00 45 00 ..S.s...t06#..E  
0010 02 0e 02 61 48 00 06 00 00 c9 a8 01 06 00 77 ...a#...F.u  
0020 f5 0c 10 97 00 50 f6 88 03 26 81 5a 06 2e 50 10 ....P...&.j.P  
0030 f8 43 3a 13 00 00 47 45 54 20 2f 65 74 08 65 72 C...GE T /ether  
0040 65 61 5c 24 6c 63 62 73 2f 6c 61 62 32 2d 2e eal:labs /lab2-2.  
0050 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 8d 0a 48 html HT P/1.1-H

Hypertext Transfer Protocol: Protocol

分組: 20 - 已顯示: 4 (20/20)

配置: Default

Yes, “IF-MODIFIED-SINCE:” and “IF-NONE-MATCH” lines are in the HTTP GET of the second HTTP GET request from the browser to the server.

The content in “IF-MODIFIED-SINCE” is same as “Last-modified”, which record the date of last modification . “IF-NONE-MATCH” is an Etag which is an identify for specific version of the resource, so when page was changed, the Etag should be changed at the same time.

## Question 4

http-ethereal-trace-2

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.337902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.537390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.548216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Frame 14: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits)

Ethernet II, Src: Dell\_Af:36:23 (00:08:74:df:36:23), Dst: Linksys6\_da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614

Hypertext Transfer Protocol

GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,\*/\*;q=0.1\r\n

Accept-Language: en-us,en;q=0.50\r\n

Accept-Encoding: gzip, deflate, compress;q=0.9\r\n

Accept-Charset: ISO-8859-1, utf-8;q=0.66,\*q=0.66\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n

If-None-Match: "1bfef-173-8f4ae900"\r\n

Cache-Control: max-age=0\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]

[HTTP request 2/2]

[Prev request in frame: 8]

[Response in frame: 33]

The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows four packets. The selected packet (No. 15) is an HTTP GET response with status 304 (Not Modified). The packet details pane on the right shows the structure of the HTTP response, including the status line 'HTTP/1.1 304 Not Modified', headers like 'Date', 'Server', 'Connection', 'Keep-Alive', and 'ETag', and the body content which is empty.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /etherreal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /etherreal-labs/lab2-2.html HTTP/1.1
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface eth0  
 Ethernet II, Src: Linksys\_Giga-Byt (08:00:27:da:a6:73), Dst: Dell\_4f:36:23 (00:08:74:4f:36:23)  
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102  
 Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 686, Ack: 1116, Len: 189  
 Hypertext Transfer Protocol  
 HTTP/1.1 304 Not Modified  
 Date: Tue, 23 Sep 2003 05:35:53 GMT  
 Server: Apache/2.0.40 (Red Hat Linux)  
 Connection: Keep-Alive  
 Keep-Alive: timeout=10, max=99  
 ETag: "1bfef-173-8f4ae900"  
 [HTTP response 2/2]  
 [Time since request: 0.022826000 seconds]  
 [Prev request in frame: 8]  
 [Prev response in frame: 10]  
 [Request in frame: 14]  
 [Request URI: http://gaia.cs.umass.edu/etherreal-labs/lab2-2.html]

The HTTP status code and phrase returned from the server in response to this second HTTP GET is 304 not modified.

No, the server didn't explicitly return the contents of the file.

Because the content of the file is not modified and there is no need to send the file again, the browser can display the locally version of the file.

## Question 5

**ETag: "1bfef-173-8f4ae900"\r\n**

The ETag value is 1bfef-173-8f4ae900.

The value of the ETag is the same in the two response message. It means that the file is not modified.

## Exercise 5: Ping Client

```
z5290005@vx2:/tmp_amd/glass/export/glass/1/z5290005/Desktop/9331 lab1/Lab2$ python3 PingClient.py lo
calhost 2000
ping to 127.0.0.1, seq = 3331, rtt = time out
ping to 127.0.0.1, seq = 3332, rtt = 195 ms
ping to 127.0.0.1, seq = 3333, rtt = 180 ms
ping to 127.0.0.1, seq = 3334, rtt = 19 ms
ping to 127.0.0.1, seq = 3335, rtt = 125 ms
ping to 127.0.0.1, seq = 3336, rtt = 113 ms
ping to 127.0.0.1, seq = 3337, rtt = 33 ms
ping to 127.0.0.1, seq = 3338, rtt = 86 ms
ping to 127.0.0.1, seq = 3339, rtt = 77 ms
ping to 127.0.0.1, seq = 3340, rtt = 88 ms
ping to 127.0.0.1, seq = 3341, rtt = 8 ms
ping to 127.0.0.1, seq = 3342, rtt = 59 ms
ping to 127.0.0.1, seq = 3343, rtt = time out
ping to 127.0.0.1, seq = 3344, rtt = 105 ms
ping to 127.0.0.1, seq = 3345, rtt = time out
The minimum rtt is 8
The average rtt is 90.66666666666667
The maximum rtt is 195
z5290005@vx2:/tmp_amd/glass/export/glass/1/z5290005/Desktop/9331 lab1/Lab2$
```